children's charities' coalition on internet safety

Briefing Note on Child Abuse Images and the Internet

This briefing has been prepared specifically to assist in the current discussions on Article 21 of the *Draft Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography*[1]. However, it is hoped the note may be of wider interest and utility.

Introduction

Without doubt the best way to stop child abuse images[2] from being circulated on the internet or anywhere else is to prevent child abuse from happening in the first place. The EU's draft Directive contains a broad range of very welcome measures to address this wider dimension.

Child abuse images are currently out on the internet where they are circulating in vast numbers and new images are being added daily. A majority of the images are published from outside the EU[3] but they nonetheless have a very real and destructive impact within it.

The images add to and magnify the injury caused by the original abusive acts depicted, and they also put the children depicted in them at risk of further harm. The images could harm other children who might be exposed to them. To the extent that the images sustain or encourage paedophile activity the continued availability of the images puts yet more children at risk in other ways.

Proven, effective technical measures exist which would allow Article 21 to be rapidly implemented. Article 21 would address the images already on the internet and discourage new ones from being posted on the web. The EU's global leadership in this field stands greatly to its credit.

Article 21 is the sole focus of this briefing note but it would be highly regrettable if the debate about how to deal with images of abuse were to dominate the entire discussion of the draft Directive as a whole. There are many other extremely important child protection challenges reflected in and taken up by the draft. Each deserves at least equal attention.

John Carr
Secretary
Children's Charities' Coalition on Internet Safety
www.chis.org.uk

July, 2010

[1] http://tinyurl.com/2asenlg
[2] This term is used rather than "child pornography" because it is felt it more accurately reflects the nature of the material
[3] http://www.iwf.org.uk/media/news.285.htm

1. Child abuse images are a visual record of abuse and humiliation

The multiple ways in which sexual abuse can damage children is well documented[4]. The internet adds to and magnifies that abuse in the following ways:

It is bad enough that a child has been sexually abused but for a record of that abuse and the attendant humiliation also to be captured then published on the internet, potentially for the whole world to see, can add to and possibly even change the nature of the psychological harm done to the child by the abusive acts shown. The permanence currently implied by an image being posted to the internet creates new and special challenges which few experts think are yet fully or properly understood.

There are some child abuse images circulating on the internet which were produced perhaps more than twenty even thirty years ago, derived from photographs or videos that have since been digitised then posted. However, the vast majority of images in cyberspace have been originated much more recently. They are linked to the emergence of cheap, easy to use high quality digital cameras, and to the development of the internet as a mass consumer product.

The newer images on the internet could have come from any of several sources, having been produced within the child's family or social circle, or procured through child prostitution. More recently there appears to have been an increase in the volume of "self-taken" still and moving images which have been obtained via web cams linked to grooming activity[5].

2. The images undermine the child's self confidence and self esteem

Child abuse images are a visual record of humiliation. The child in an image that has been uploaded to the internet can never know, never be certain, who might have seen or downloaded it, or who might be about to. It severely undermines the child's self confidence and gnaws away at their self esteem. Every casual glance or remark, for example from a stranger on a bus, potentially can be interpreted through the prism of the possibility, the anxious embarrassing worry, that this other person has recognised them from the picture .

As a distinguished clinician in the field has put it[6]

The distribution of child sex abuse images means there can be one victim and many offenders. The fact that these images are spread and downloaded by others leads to heightened symptoms of post traumatic stress disorder, depression and or anxiety, plus a diagnosis so far not commonly seen in child sex abuse cases – paranoia.

3. The images are a gross violation of the child's right to privacy

In any and all proceedings concerning the abuse of a child, the courts and the professional staff working with the child go to extraordinary lengths to preserve the anonymity of the victims. That is rooted in sound therapeutic principles. If nothing else, the production and publication of child abuse images on the internet should be considered as a gross violation of the child's right to privacy. By definition there can have been no question of consent.

---

[4] See for example http://tinyurl.com/ecmsexp Safeguarding Children and Young People from Sexual Exploitation, DCSF, June 2009, page 22

[5] http://tinyurl.com/ceoppage22 at page 22

[6] Dr Sharon Cooper, MD FAAP, University of North Carolina Chapel Hill School of Medicine, USA

4. Preventing further publication is a very important child protection measure

The fact that a child knows or believes images of their abuse remain on and continue to be spread by the internet can lead to ever greater feelings of helplessness.

Therapists and counsellors who work with abuse victims whose images have appeared on the internet[7] therefore agree it can help the child enormously to regain some sense of control over their lives, and immeasurably improves their chances of getting on to a path to some sort of recovery, if they are seen to be believed about the abuse they have suffered and the child understands and accepts that everything possible is being done, as fast as possible, to stop more people being able to look at those pictures.

If the abused child cannot be truthfully told or promised that no more new people will see the pictures, and that will rarely be possible, then they can at least be comforted and helped by knowing that everything that can be is being done, again as quickly as possible, to stop or limit the images spreading. As another distinguished clinician put it

If we as clinicians do not convey to the child that we are doing everything in our power to stop further distribution of the images, we send the wrong signals to the child and may strengthen destructive patterns.[8]

Of course removing the pictures from public view is not the be all and end all of the matter. As the same clinician observed

On the other hand if we convey the sense that it is absolutely necessary to stop all further distribution for the child ever to feel OK about herself or himself again we end up in another corner and may disrupt the healing process. Working with accepting the consequences of a crime committed towards the child must always be connected with a clear message and a clear stand against the injustice committed against the child. And such a stand must also always be followed by actions. Thus I believe the disruption of distribution of the images to be a key factor in the recovery process but it is not the only or necessarily the main factor.

5. Further or repeated publication of the images re-abuses the child

For as long as the images remain on public view on the internet the abused child is in a very real sense being "re-abused" and being put at risk of further harm. It is also why people who deliberately engage in viewing or downloading these images are in reality child abusers by proxy. A survivor of abuse that was recorded in photographs put it like this:

Those who view the images of my abuse are no different from those who made them in the first place. It feels like they are in the room, encouraging my abuse. I know, technically, there is a difference but, for me, it's not a lot of difference[9]

6. Further or repeated publication risks creating new child abusers

There is a growing body of evidence which suggests that people who deliberately download and start collecting child abuse images are significantly more likely than the general population to commit offences[10] against children, either online or in the real world, or both[11].

---

[7] Tink Palmer, Marie Collins Foundation, UK, Julia von Weiler, Innocence in Danger e. V, Germany.
[8] Bengt Söderström, psychologist, Stockholm Child & Adolescent Psychiatry
[9] Marie Collins, Marie Collins Foundation, Dublin
[10] That is additional offences since the act of downloading the images is also an offence

Not all downloaders will be equally dangerous to children, and many will not reoffend once caught, particularly if they are helped to manage their future behaviour and are supported by appropriate forms of monitoring or supervision. However great caution is nonetheless always required because of the difficulties associated with predicting how any given individual might behave in the future. Images can fuel downloaders' fantasies, spurring them on to commit further illegal acts. That is the second major reason for wanting such images to be removed from view as quickly as possible: it helps reduce the number of potential new online and offline child abusers. To the extent that images also sustain or encourage paedophile activity the availability of the images clearly puts yet more children at risk in other ways.

7. What is known about offenders?

Repeated studies have shown that conventional stereotypes of "typical" child sex offenders or "typical" downloaders of child abuse images are unhelpful and inaccurate. Such stereotypes conceal more than they reveal, acting as a barrier to understanding. People who engage in these activities come from all walks of life and from every kind of cultural background.

The National Society for the Prevention of Cruelty to Children (NSPCC), a leading children's organization in the UK and a CHIS member, carried out an analysis of 100 cases where convictions for offences related to child abuse images had been obtained in courts in England and Wales between September 2008 and March 2010[12]. This was not by any means all of the cases that had gone to court during that period. It was just a sample of cases that had been reported in the media. By way of context, the total number of cases where convictions for the same offences had been obtained in 2007 in courts in England and Wales was just over 1,400. The 100 cases used in the NSPCC study therefore cannot be said to be a representative sample. They provide only a snapshot of the total, but these 100 cases show features which constantly reoccur in others.

The 100 cases involved 99 men and one woman. Two of the offenders had been collecting images for more than ten years prior to their arrest, another eight had been collecting for more than 5 years. 16 of the offenders had concurrent or previous convictions for sexual assault on a child or for grooming a child for sex. A further 5 offenders were reported to have fantasised about abusing a real child in chat room conversations. 5 of the offenders had contacted or attempted to contact a child online. One of these had gone on to abuse the child he had made contact with. 24 of the 100 offenders were in positions of trust within their communities: 7 were teachers or school employees, 6 were doctors, nurses or hospital staff, 5 were clergy or church volunteers, 2 were police officers, one was a tennis coach, another a prison officer in a young offenders' institution, one was a social worker and another worked in a children's residential care establishment.

8. Removal of the illegal images by deletion is the preferred option

For the reasons given it should be clear why there is a concern to ensure that, once discovered, any child abuse images are taken down and removed from public view as swiftly as possible. Linked to this there should always be a law enforcement investigation to determine who was responsible for producing and distributing the material so they can be held to account.

---

[11] See for example, *Self-Reported Contact Sexual Offenses by Participants in the Federal Bureau of Prisons' Sex Offender Treatment Program: Implications for Internet Sex Offenders, Hernandez, November 2000*, presented at the Association for the Treatment of Sexual Abusers (ATSA) in San Diego, California; also *From Fantasy to Reality: The Link Between Viewing Child Pornography and Molesting Children*. *Kim, C (2004)*, based on data from the US Postal Inspection Service, *Kim, C*; and *Internet traders of child pornography and other censorship offenders in New Zealand: Updated Statistics (November 2004), Wilson and Andrews.*

[12] http://tinyurl.com/nspccstudy

However, where deletion at source cannot be done swiftly, blocking can play an extremely valuable role. Blocking is a legitimate, necessary, tactic to disrupt the trade in or display of images whilst the perpetrators are investigated and while the administrative or other processes move forward to have the material permanently deleted at source.

9. What is blocking?

To delete an image at source normally requires direct access to the server or site on which it is housed. Such access is usually only available to the owner of the server or whoever administers the site. These owners or administrators can be hard to locate, reluctant to co-operate or there may be other barriers which impede or delay removal[13].

Blocking is the next best thing to deletion. Blocking involves deploying technical measures, typically at network level by an Internet Service Provider (ISP)[14], to deny users access to child abuse images. In most EU Member States blocking systems are based on a list of pre-identified sites or addresses. The list is normally constructed and maintained by the police. In the UK it is constructed and maintained by the Internet Watch Foundation (IWF), the UK's hotline[15], a body that works very closely with and is supported by the police[16].

Thus, blocking in and of itself does nothing to ensure the material is permanently removed from view. The illegal material will stay up until it is deleted by the owner or administrator and therefore it could still be reached and viewed or downloaded by persons who can gain access via another internet connection where no blocking is being applied[17]. Alternatively the illegal material could be reached in other ways providing the individual looking for it has the right level of technical knowledge and sufficient determination[18].

The Italian experience shows it is possible to act against illegal images at great speed[19], but outside of Italy in multinational cases this is simply not happening at the moment. It never has and there is no suggestion that this position can or is going to change within any kind of acceptable timeframe.

Academics from the University of Cambridge have shown[20] that, in reality, once a report of the location of an illegal image has been made to the appropriate authorities in an overseas jurisdiction the material can nonetheless still stay up, waiting to be deleted by the owner or administrator, for substantial periods of time, months, or even years. The work of the Cambridge dons is confirmed on an on-going basis by the daily experience of those hotlines around the world who make reports about

---

[13] See http://www.cl.cam.ac.uk/~rnc1/takedown.pdf, "The Impact of Incentives on Notice and Take-down", Moore and Clayton

[14] Search engines also do something similar to block access

[15] A "hotline" is an organization or a mechanism which allows anyone to report the address of any content which they find online that they believe is illegal. INHOPE, www.inhope.org is the global association and standard setting body for hotlines.

[16] Technically the IWF is an NGO and it is also a charity. The IWF is funded principally by the internet industry although it also receives support from the EU's Safer Internet Programme. The UK police typically ask people to report all illegal child abuse images to the IWF in the first instance. The IWF screens out incorrect referrals before passing confirmed cases to the police for investigation.

[17] In the UK 98.6% of everyone with an internet connect in their home is with an ISP that does blocking.

[18] The number of people who have the knowledge and determination is hard to determine (see following section) and if every country in the world were doing blocking there would be far fewer or no alternative addresses for people "to circumvent to"

[19] In Italy by law once notified by the police ISPs have six hours to remove or block access to identified illegal material or addresses.

[20] Moore and Clayton, *ibid.*

sites they have previously reported, perhaps on many occasions. Some small scale experiments are being attempted which involve contacting the owners of the servers or site administrators directly but it is far from clear that this can scale to the required level.

10. The importance of the web

The emergence of the web completely transformed and hugely enlarged the "market" for child abuse images[21]. Prior to the arrival of the internet, in most parts of the world it was extremely difficult to get hold of child abuse images. A person interested in acquiring any usually had to know someone else who already had some or else go to great trouble and take several risks. Even as recently as the mid 1990s one distinguished expert on child protection was able to describe the exchange of child abuse images as being "a cottage industry"[22]. Today the images can be a mouse click away. It is a global industry worth millions of dollars to those who engage with it for financial gain[23].

Taking 1995 as "Year 0" (the last year before the Internet boom erupted in many countries), Interpol say at that time they knew of around 4,000 child abuse images in total[24]. The British police say that in 1990 they were aware of 7,000 unique images[25]. The numbers of children depicted in these images could be counted in hundreds. Data recently supplied by Interpol and other data published in the UK[26] and Italy[27] suggest that today the number of known unique images is around 1,000,000, and the number of children abused to make them runs into the tens of thousands[28]. There is a marked growth in images of younger children being subjected to ever more violent and depraved sexual acts.[29] It is anybody's guess how often the images and their duplicates are downloaded or exchanged online and off, but it is very likely to run into billions per annum.

Another indication of the change in the scale of modern offending comes from an examination of the numbers of images seized by the police when arresting suspects. Prior to the Internet, typically police officers would arrest individuals with only a handful of images in their possession, or in unusual cases maybe hundreds. In the whole of 1995 the police in Greater Manchester in the UK seized the grand total of 12[30] whereas a few years later the same force, covering broadly the same population arrested one man, John Harrison of Denton, with approximately 1,000,000 images in his possession[31]. In June 2009 in a single action the police in Mexico arrested one man, Arthur Leland Sayler, who possessed 4 million images.

The trend in convictions is another useful signifier. Taking 1995 once more as the baseline, in the UK[32] 142 people were cautioned or proceeded against for child abuse image offences. In 2007 it was 1,402.[33] Precise comparisons between 1995 and 2007 in terms of Internet usage

---

[21] "Child abuse, child pornography and the internet", John Carr, http://tinyurl.com/cacpint.
[22] *People Like Us*, Sir William Utting, HMSO, London, 1997
[23] See http://www.justice.gov/opa/pr/2001/August/385ag.htm where "In just one month, the (web site) grossed as much as $1.4 million."
[24] Correspondence with author
[25] http://www.official-documents.gov.uk/document/cm77/7785/7785.pdf, page 7
[26] http://www.official-documents.gov.uk/document/cm77/7785/7785.pdf, page 8
[27] Telefono Arcobaleno speak of 36,000 children of whom '42% are under 7 years of age and 77% are under the age of 12' www.telefonoarcobaleno.org/pdf/tredicmoreport_ta.pdf
[28] And bear in mind these numbers and are based solely on what is known about through successful police actions. The true volumes are likely to be higher.
[29] See http://preview.tinyurl.com/iwfreppage8, page 8
[30] Correspondence with the author
[31] http://tinyurl.com/manchestermillion
[32] It proved impossible in the time and with the resources available to obtain reliable comparable data from other jurisdictions.
[33] Offending and Criminal Justice Group (RDS), Home Office, Ref: IOS 503-03

are not very meaningful because broadband barely existed in 1995, while by 2007 it had become commonplace.[34] In 1995 fewer than two millions UK households had (primarily dial-up) Internet access, whereas by 2007 the number of households with Internet access was up to 15.23 millions, of whom 84% had broadband.[35] The inference is pretty clear. There is a strong link between Internet crimes of this kind and the growth in the number of broadband Internet connections within a country. No nation appears to be exempt.

The little evidence there is about the profiles of people arrested for downloading child abuse images suggests that the majority were not especially technically literate or competent. One expert[36] calculated that "at least half" of the men he deals with could very easily have been deterred from seeking out child abuse images if they had been put behind almost any kind of technical barrier such as web blocking. The fact that some highly motivated and highly technically literate offenders can circumvent a particular measure is no reason to abandon that measure altogether. Look at the continuing battle against spam and viruses.

If a significant number of potential offenders e.g. "at least half", can be prevented from becoming engaged with child abuse images, it promises to free up law enforcement's time and resources to allow them to track down and deal with the smaller numbers who are clearly very determined to find the images and who also have the technical knowledge so to do.

11. Other technologies present different challenges demanding different solutions

The web remains by far the most popular and most widely used internet interface and that is why it is so important to deal with it. However, web blocking does not touch other technologies that are also used to distribute child abuse images. Most obviously there is a need to address the issue of Peer2Peer software and the re-emergence of Usenet Newsgroups as repositories for child abuse images. Tackling these requires separate, additional measures. It is not a choice between tackling them *or* tackling the web. They are not alternatives. Both are needed. Each requires specific and discrete approaches. The widely held view is simply that the web remains the most important internet interface and therefore, if there has to be a queue or choices have to be made, the web should be at the top of the list.

A study by the Australian Computer Society[37] suggested that 96% of all offenders convicted for child abuse image offences had found or distributed images using the worldwide web. 50% of offenders had also used Internet Relay Chat (IRC), 43% had also used Peer2Peer, email had been used by 23% of offenders and File Transfer Protocol (FTP) was used by 12% of offenders. These numbers both reinforce and underline the importance of the web as a medium of exchange but they also make it clear that dealing with the web alone is not enough.

In the NSPCC study referred to above, in 37 out of the 100 cases Peer2Peer or similar filesharing programmes were directly referred to in the court proceedings[38]. This does not prove that Peer2Peer is more or less important than the web but it does show that the web continues to be important.

Locking out the producers and distributors of child abuse images from online payments systems is also vital[39]. The IWF only engages with content on the web. It reported in May, 2010, that in 2009

[34] Broadband access is important because it facilitates rapid and cheap access to large files. Typically child abuse images and videos will be large files.
[35] http://www.statistics.gov.uk/pdfdir/inta0807.pdf
[36] Donald Findlater, Lucy Faithfull Foundation
[37] Technical Observations on ISP based Filtering of the Internet", www.acs.org.au/ispfiltering; p8
[38] This does not mean Peer2Peer programmes were definitely not used in any of the other 63 cases looked at. It just means there was no reported reference.

they had acted against 1,316 web sites in all parts of the world, and had identified 450 distinct "criminal brands" that were selling images of the sexual abuse of children worldwide.

ICANN[40] and their associated TLDs[41] should formulate policies and strengthen their procedures for ensuring that the domain names system cannot be used to promote or advertise sites which provide access to child abuse images, or which regularly contain such images or disseminate information about where to obtain them. In addition ICANN should move swiftly to implement the due diligence proposals made by the GAC[42] at the June, 2010 meeting in Brussels to establish a global requirement for all Registrars and their agents to verify the name and address of everyone applying for a new domain and everyone wishing to maintain an existing one. The payment details relating to any domain registration should also be confirmed as being authentic and legitimate. IANA[43] should also formulate policies and procedures which should be applied globally to allow for the removal of previously allocated IP addresses where it can be shown[44] that these addresses are being persistently used for criminal purposes.

12. Huge numbers of illegal attempts to locate child abuse images are made every day

The importance of blocking becomes apparent when one examines the available evidence on the scale of the attempts being made to reach known addresses containing child abuse images on the web.

In 2009 BT announced that they had estimated that, over their broadband network, their blocking solution was preventing up to 40,000 attempts per day to access web sites known to contain child abuse web images. Extrapolated across the whole of the UK broadband network this suggests that blocking is preventing up to 58 million attempts per year[45]. Five months after blocking was launched in Denmark in 2006 the Danish police estimated that 238,000 users had attempted to reach known illegal child abuse images on the web[46]. It was estimated that in Norway blocking was stopping between 10 and 12,000 attempts per day and in Sweden it was in the order of 20 – 30,000 per day[47]. These are substantial numbers.

The Danish police referred to the number of users who had attempted to reach the illegal addresses, but the UK, Norwegian and Swedish numbers refer to *attempts*, many of which will be machine based e.g. emanating from web crawlers or botnets, but even so each and every attempt whether by a human or an automated system represents a criminal act of some sort.

13. An international problem calls for international solutions

The majority of child abuse images on the web are housed on servers in countries outside the EU[48]. This does not mean the children depicted are necessarily from outside the EU. Neither does it mean the people responsible for the abuse, for photographing, filming or putting it on the internet are inevitably from outside the EU. Just as it is often very hard to know where the children in the images or videos are from, it is also difficult to know where the perpetrators or distributors are based.

---

[39] The European Financial Coalition, http://www.ceop.police.uk/efc/ is working on this aspect along with its US based counterpart the Financial Coalition Against Child Pornography, http://tinyurl.com/icmecrep

[40] The Internet Corporation for Assigned Names and Numbers, www.icann.org

[41] Top Level Domains

[42] Governmental Advisory Committee

[43] Internet Assigned Numbers Authority, www.iana.org

[44] For example through court records where convictions have been obtained

[45] http://www.theregister.co.uk/2009/04/07/bt_cp_figures/

[46] http://www.politi.dk/da/aktuelt/nyheder/2006/boernepornofilter_24052006.htm

[47] http://www.politi.dk/da/aktuelt/nyheder/2005/filter_181005.htm

[48] http://www.iwf.org.uk/media/news.285.htm

The universal reach of the internet means, in any event, it is no longer morally possible to confine safeguarding activities to children living within the geography of local national or regional boundaries. Wherever the images are being housed or published from, the presence of these images on the internet can have a very direct and destructive impact within the EU, in the ways described earlier. That is a key part of the justification for the Commission's proposal.

Part of the problem is that, in the countries where the illegal images are being hosted, the decision to investigate the source, or the decision to issue a notice to get the material deleted or taken down, is normally left to hugely over-worked police departments that may sometimes be preoccupied with what they consider to be more pressing domestic policing issues. Even if that were not the case, the capacity of or resources available to some police forces may already be severely stretched, making participation in any kind of complex international investigation or operation impossible.

Thus, if the case has not been reported to the local police from an agency or a person within their own jurisdiction, there may be a temptation for law enforcement to put the request towards the bottom of their already huge In Tray. Even within the EU, between Member States, this can happen. This is why it is important to support amendments to the draft Directive to impose specific obligations on EU Member States. Police forces and other relevant agencies need to respond swiftly to lawful and legitimate take down notices, irrespective of the jurisdiction in which they originated.

To support and recognize this multinational dimension consideration should therefore be given to creating a new international investigative unit which can work with, and will win the engagement of, all the relevant national and other policing units or agencies working in the field. The crucial point is that such an internationally based unit will not be the subject of the same local demands or pressures that can inevitably and understandably press in on police organizations which are wholly based within one country. Presented properly the overwhelming majority of national police agencies will recognize the value of such a unit and appreciate that it can provide them with extra specialist help and support.

14. Other international instruments may also help move this agenda forward

In addition to the measures already referred to there is clearly also scope for the EU to use a range of international instruments e.g. diplomacy, trade negotiations, trade agreements or other forms of treaties, to reinforce the importance it attaches to winning international co-operation for a comprehensive, thorough and much swifter international notice and take down regime, thus reducing any dependency on or need for blocking systems.

However, even with the best will in the world and at full sail, international diplomacy and treaty negotiations can move at glacial speed. For this reason it is not right or acceptable to ignore a solution that can make a significant contribution and is available right now, against the hope that such diplomatic endeavours will be able to deliver a significant shift in policy and practice on any sort of near time horizon.

Just as the EU can utilise the tools of diplomacy so too, of course, can individual Member States in any bilateral or multilateral dealings they might have with third parties.

15. Improvements in locating, identifying and helping victims are needed

The importance of every case being fully investigated by law enforcement has already been commented upon above. However it is readily acknowledged that finding the children depicted in the images is often a tremendous challenge.

Technical improvements in the ability of different police held databases to work together may lead to more efficient, speedier efforts to determine the whereabouts of victims depicted in images but it is obvious that, usually, before a serious investigation can even begin it is necessary, or at any rate

highly preferable, at least to have an idea about the country or jurisdiction where the offence shown took place. Unless the producer of the image has, normally unwittingly, left a clue about the geography it can be hard to make any real progress. Improved analytical tools are likely to have an important role to play in this area.

Once a child has been identified and located decisions need to be taken about the best way to intervene to rescue the child and put him or her on to a road to recovery. A partnership approach is likely to be critical to ensuring that the needs of the child are always paramount. In particular the law enforcement needs to be fully engaged with the partnership. Law enforcement systems need to value the role and importance of child protection.
Linked to this, it is important to have a trained workforce that both understands and knows how to respond effectively to children whose abuse has been circulated on the internet or children who may currently be experiencing other forms of internet related abuse.

16. Vital to reduce the possibility of the images reaching their intended markets

The criminal networks behind many of the commercial child pornography web sites typically are often not run by people who could not be classed as paedophiles in the ordinary sense. They systematically arrange for children to be raped by others solely in order to photograph and film the rape as a prelude to selling the pictures of it for profit.

If these gangsters cannot reach a large part of their market, through the web, or if they are unable to collect payments for the images because the banks and credit card companies have locked them out, they will stop doing it or at any rate the volumes will be reduced as their trade is disrupted or closed down. Fewer new children will be abused, fewer children who have already been abused will be re-abused by their images remaining on display and fewer new people will find the sites thus reducing the risk of creating new child abusers.

By contrast if it is seen that this type of illegal activity can survive and prosper on the internet, it may encourage new people to come into "the market" and thereby add to the spiral of abuse of children. It might also encourage or spread a belief that the internet is a safe place to engage in different kinds of crimes. Attacking the presence of child pornography on the internet is therefore not only important in its own right, it is also a key part of building trust and confidence in the internet more generally.

17. Worries about "mission creep" must be addressed

A number of concerns have been expressed about the way web blocking could be misused for other purposes. This is sometimes called "mission creep".

The political importance of this point must be recognized and it therefore has to be properly addressed but in and of itself the argument has little intellectual or ethical substance.

Each case should be taken and judged on its merits. It is absurd to say that because some technologies *could* be used or are being used in bad ways by bad people, that good people should never even think about trying to use them to do good things. If this logic was applied to scientific research or progress in any number of areas it would bring many things to a halt.

It is morally indefensible to refuse to engage with blocking child abuse images simply because of real or imagined worries about how other governments or other organizations might twist or misuse the same or similar arguments or twist or misuse the technology for other less elevated purposes. The EU has to do what it thinks is right.

The protection of child abuse victims should never be a contingent factor in other people's arguments about something else. If individuals believe it is wrong, for example, to use web blocking technology against gambling sites or sites that provide access to copyrighted music or videos, then they should say so and vote against whenever and wherever possible, but they ought not to make abused children pay for it. Child protection is not a bargaining chip.

It is of course true that some governments suppress free speech on the internet within their country or deny their citizens access to information by using blocking. However, that does not invalidate or compromise a legitimate use of blocking for lawful and good purposes. All of the materials that would be blocked under Article 21 of the draft Directive are by definition illegal items. If they were not illegal there would be no basis for blocking them or for them being on anybody's list.

18. The technical measures and surrounding systems used

There are several ways of implementing a blocking system. Some of them are exceptionally crude and carry with them a very high risk of doing collateral damage, of over-blocking i.e. of preventing access to perfectly legal and legitimate web addresses.

On the other hand there are more sophisticated technical measures available which for all practical purposes carry a level of risk of over-blocking which is at or very close to zero. The children's organizations favour the more sophisticated systems and strongly oppose the older, cruder versions.

The children's organizations are strong supporters of free speech and free expression. In their daily work they constantly encourage children and young people to be active participants in and engaged citizens of the democratic life of their country. Thus not only do the children's organizations oppose any attempts to interfere with or restrict free speech or free expression in principle, they also condemn the use of systems which, for whatever reason, trample on or disregard other people's rights, thereby undermining the legitimate case for the highly targeted blocking of child abuse images.

Moreover when implementing any system to take forward blocking it is also important that close attention is paid to the security of all the systems surrounding the construction, storage or distribution of blocking lists.

19. Democratic accountability and scrutiny are essential

Underlying aspects of people's anxieties about "mission creep" is often a related concern that the use of blocking technology is open to abuse. It should be expressly noted that the draft proposal currently being debated within the EU only provides authority for blocking access to child abuse images. It does not provide any authority for blocking anything else. Nonetheless some people are concerned that, should blocking system be established, access to web sites could be blocked surreptitiously, for political or commercial reasons.

If systems were to be misused for other unauthorised purposes it would, of course, be illegal. However, precisely because there are legitimate fears about improper censorship, it is completely accepted that the way in which blocking is carried out must be the subject of transparent policies and procedures. It should not be possible for any reasonable person to harbour any reasonable doubt or suspicion about the way the list of sites to be blocked is constructed, maintained or used.

Thus every aspect of the construction and operation of a blocking list must be open to judicial review. In the UK the IWF maintains and manages the list. The IWF is subject to judicial review and in addition its operations are subject to full and regular scrutiny by respected, independent external experts.

If an internet address is blocked the reasons why it has been blocked should be stated and there should be an appeal mechanism. The draft of Article 21 makes provision for that. It says:

The blocking of access shall be subject to adequate safeguards, in particular to ensure that the blocking is limited to what is necessary, that users are informed of the reason for the blocking and that content providers, as far as possible, are informed of the possibility of challenging it.

20. Working within a framework of the rule of law is fundamental

To address the gigantic growth in the number of child abuse images being distributed over the internet a modern jurisprudence which is fit for purpose is needed. Many analogue solutions simply do not work in the digital world. Typically the problems being confronted are rooted in the speed, scale or the complexities which inevitably arise from the international nature of cyberspace or more likely some combination of these.

If passed in roughly its present form the Directive would not require every Member State to act in exactly the same way but it would constitute a new EU-wide minimum or uniform law, creating a new baseline. UK law already complies with or exceeds the anticipated new minimum and therefore will continue to include items which are not regarded as illegal in some jurisdictions[49].

Judicial and investigative processes sometimes feel as if they are stuck in the mid to late 20th Century whilst the rest of us are already well into the 21st. Thus, given the volumes involved, the suggestion that only a judge or a court can declare whether or not a particular image is illegal is either an argument for vastly increasing the number of judges, courtrooms, lawyers and investigators societies must collectively employ or it is an argument which says, effectively, there is little or nothing that can be done other than learn to live with an ugly new reality. Civilized society is not ready to concede the latter position.

The case referred to earlier of Arthur Leland Sayler, arrested in possession of 4 million child abuse images, was an extreme example but finding individuals with hundreds of thousands of images on their machines is an everyday event for police forces across the world. Finding someone with a million images no longer guarantees a newspaper headline. Some level of extra judicial, but quasi judicial, processes have to be allowed to develop to cope with the new quantum. There was a time when only police officers could issue parking tickets. Those days are long gone in most cities, but ways still exist to appeal against one which is thought to have been issued wrongly.

Moreover, in relation to blocking, the relevance of the point about judicial processes is not clear. If an apparently illegal image is published within the same jurisdiction as the finder the question of it appearing on a blocking list in that country will never arise. However, where someone in country X finds an image that is being hosted in country Y, it seems far fetched to suggest that a judge in country X has to make an adjudication before the URL containing the image can go on a blocking list to be deployed in country X. Even more judges, lawyers, courtrooms and investigators will be needed.

Article 21 brings the use of blocking clearly within the framework of law and that includes the potential for judicial review if there is any evidence that something is not right.

Article 21 and the draft Directive as a whole deserve widespread support.

---ooo---

[49] See Crown Prosecution Service guidance at http://tinyurl.com/cpsrules